SIEMENS

PATENT
Attorney Docket No. 2002P15289WOUS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Inventor:	M. Franke et al.	)	Group Art Unit: 2434
		)	
Serial No.:	10/528,312	)	Examiner: Hailu, Teshome
		)	
Filed:	03/17/05	)	Confirmation No.: 2692

Title: METHOD FOR GENERATING AND/OR VALIDATING ELECTRONIC SIGNATURES

Mail Stop Appeal Brief - Patent
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450
COMMISSIONER FOR PATENTS

APPELLANTS' BRIEF UNDER 37 CFR 41.37

Sir:

This brief is in furtherance of the Notice of Appeal filed in this application on 9 July 2009. It is also in furtherance to the first Appeal Brief filed 23 July 2008 because the application was withdrawn from appeal in the Office Action mailed 20 October 2008. The prior appeal contested rejections under Section 103 based in part on the Oka reference (U.S. 2002/0108042) while this appeal traverses rejection of the same identical claims under Section 102 based on the Oka Reference. The additional fee required for submittal of this brief due as a result of a change in the fee requirements is authorized herewith.

1. REAL PARTY IN INTEREST - 37 CFR 41.37(c)(1)(i)

The real party in interest in this Appeal is the assignee of the present application, Siemens Aktiengesellschaft.

2. RELATED APPEALS AND INTERFERENCES - 37 CFR 41.37(c)(1)(ii)

There is no other appeal, interference or judicial proceeding that is related to or that will directly affect, or that will be directly affected by, or that will have a bearing on the Board's decision in this Appeal.

3. STATUS OF CLAIMS - 37 CFR 41.37(c)(1)(iii)

Claims canceled: 1 - 5, 7, 9, 11, 13, 15, 17, 19 and 21.
Claims withdrawn but not canceled: None.
Claims pending: 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23.
Claims allowed: none.
Claims rejected: 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23.

The claims on appeal are 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23. A copy of the claims on appeal is attached hereto in the Claims Appendix. Appellants respectfully appeal the final rejection of claims 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23.

4. STATUS OF AMENDMENTS - 37 CFR 41.37(c)(1)(iv)

In response to the Final Office Action mailed 10 April 2009, the Appellants submitted a response without amendment under Rule 116 on 10 June 2009. The Examiner entered the Response per the Advisory Action mailed 25 June 2009. The Advisory Action indicates that the grounds of rejection presented in the Final Office Action remain unchanged.

5. SUMMARY OF THE CLAIMED SUBJECT MATTER- 37 CFR 41.37(c)(1)(v)

With reference by page and line number to the detailed description, the following summary references one or more exemplary embodiments described in the Specification and which are covered by specific claims, but it is to be understood that the claims are not so limited in scope.

5A. BRIEF BACKGROUND PROVIDING CONTEXT FOR THE SUMMARY OF CLAIMED SUBJECT MATTER

The invention relates to electronic signatures of the type used to assure authenticity, legal validity and integrity. Such signatures generally require two keys which are mathematically dependent on one another. A private key is used for generating the electronic signature. A public key is used for verifying the signature provided, i.e., by identifying a link between the name of the person to whom the signature relates and the corresponding public key. This link, referred to as a certificate, is issued by a third party, referred to as a certification authority.

Certificates only have a limited period of validity. Certification authorities have separate key pairs for signing certificates, creating black lists and time stamps. Signature methods have included a first algorithm for generating the signature and an associated second algorithm for verifying signatures.

Prior known signature methods have required significant effort to effect permanent protection of the private signature key (by the person to whom the signature is assigned) against unauthorized use. The claimed invention relates to generation of electronic signatures without requiring permanent protection of the private signature key by the person to whom the signature is assigned.

According to an embodiment of the invention, certification of the public validation key need not take place until after calculation of the electronic signature. An intentional action by an author of an electronic document (e.g., expressed by use of the electronic signature) may only take place after signature generation in the context of a certificate request process. Because the intentional action is represented by a certificate request (instead of an initiation of a calculation of an electronic signature) it is not necessary to keep a private signature key which corresponds to the public signature key after calculation of the electronic signature. Consequently, the private

signature can be destroyed following a calculation of the electronic signature. Therefore a need no longer exists for protecting the private signature key against unauthorized access.

Also according to embodiments covered by the claims, when validating an electronic signature only those signatures which were generated at a time prior to the certification of the public validation key are recognized as valid. This has the result of eliminating the revocation problems which relate to public validation keys and are known in the context of previous signature methods. Moreover, this ensures that it is no longer possible to misuse the private signature key after the time of the certification of the public validation key. Therefore no mechanisms for permanently preventing unauthorized accesses to the private signature key are required.

When certifying the public validation key in accordance with the claimed invention, it is possible to include a reference to the relevant signed electronic document in addition to a user identifier and the public validation key. When validating the signature on the recipient side, the reference to the electronic document is also evaluated. Furthermore, it is possible for the certification of the public validation key to include not just one reference to a single electronic document, but a plurality of references to electronic documents which are signed within a specific reference period. A reference to an electronic document may be implemented, for example, by means of a calculated hash value for the relevant electronic document. When validating signatures on the recipient side, corresponding hash values are compared.

5B. CONCISE EXPLANATION OF SUBJECT MATTER DEFINED IN EACH INDEPENDENT CLAIM

5B(i). Summary of Subject Matter Defined In Independent Claim 6.

In accord with Figure 2, **independent claim 6**, directed to a method for generating or validating electronic signatures, includes the steps of

(i) generating an asymmetrical key pair (Step 200) which includes a private signature key 210 and a public validation key (see page 6, line 28 - page 7, line 1; and page 7, lines 7-10);

(ii) calculating an electronic signature for an electronic document by means of the private signature key and by applying a predeterminable signature function (see again page 6, lines 30 - page 7, line 1); and

(iii) performing a certification of the public validation key (see page 7, lines 7 - 30) wherein, when validating, only those signatures generated at a time prior to the certification of the public validation key are recognized as valid. See page 7, line 32 - page 8, line 9.

5B(ii). Summary of Subject Matter Defined In Independent Claim 18

Also in accord with Figure 2, **independent claim 18** is directed to a method for generating or validating electronic signatures. The method includes

(i) generating an asymmetrical key pair (Step 200) which includes a private signature key 210 and a public validation key (see page 6, line 28 - page 7, line 1; and page 7, lines 7-10);

(ii) calculating at least one electronic signature for at least one electronic document by means of the private signature key and by applying a predeterminable signature function (see again page 6, lines 30 - page 7, line 1); and

(iii) following calculation of the electronic signature, of which there is at least one, carrying out a certification of the public validation key wherein only those signatures generated at a time prior to the certification of the public validation key are recognized as valid. See page 7, line 1 - page 8, line 9.

6. GROUNDS OF REJECTION TO BE REVIEWED UPON APPEAL - 37 CFR 41.37(c)(1)(vi)

Whether claims 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23 are unpatentable under 35 U.S.C. Section 102(b) as being anticpated by U.S. Pub. No. 2002/0108042 (Oka).

7. ARGUMENT 37 CFR 41.37(c)(1)(vii)

7A. APPELLANTS TRAVERSE THE ART REJECTIONS.

With Regard to the Art Rejections, Patentability of Each Claim is to be Separately Considered

Appellant urges that patentability of each claim should be separately considered. All of the claims are separately argued. General argument, based on deficiencies in the rejection of independent claims 6 and 18 under Section 102 demonstrates patentability of all dependent claims. However, none of the rejected claims stand or fall together because each dependent claim further defines a unique combination that patentably distinguishes over the art of record. For this reason, the Board is requested to consider each argument presented with regard to each dependent claim. Argument demonstrating patentability of each dependent claim is presented under subheadings identifying each claim by number.

7A. REJECTION OF THE INDEPENDENT CLAIMS 6 AND 18 IS IN ERROR.

The Appellants traverse all of the claim rejections under 35 USC 102 because the Oka reference used to reject independent claims 6 and 18 fails to disclose each feature recited in the claims.

7A(i). REJECTION OF INDEPENDENT CLAIM 6 UNDER SECTION 102 BASED ON OKA IS IN ERROR.

Application of the Oka reference under Section 102 results in deficiencies that render the rejection of claim 6 incorrect. The method of claim 6 requires **performing a certification of the public validation key wherein, when validating,**

"only those signatures generated at a time prior to the certification of the public validation key are recognized as valid."

In arguing the rejection the final office action does not account for the word "only" which requires that, for a signature to be valid, the signature must be generated prior to the time that the public validation key is certified. Instead, the rejection incorrectly refers to Oka at page 12 (par

193) and Figure 22 to assert that the above recitation (from claim 6) reads upon this prior art. Specifically, the rejection notes that the example (see pars 192 – 203 of Oka) is a series of steps 1 – 10 in ascending order. The rejection cites step 8 of Oka (par. [0201]) which only concerns validation of a signature on a received public key certificate. Without support for doing so, the rejection concludes that because step 8 determines whether a signature on a public key certificate is valid, and step 9 (par. [0202]) sends a signed certificate to the registration authority, the terms of the above-quoted recitation are somehow met. Yet this is not what claim 6 requires.

Rather, the above-quoted recitation from claim 6 does not relate to step 9 (sending "a signed certificate to the registration authority"). Instead, the above recitation refers to signatures generated on documents prior to the *certification of the public validation key.* On the other hand, step 5 of Oka specifies that the "signature generation instruction" is command and message data *for a certificate to be generated* (see par 198); and step 6 expressly states that this same instruction is executed. Thus **the certificate is generated in step 6.** The fact that the certificate is generated in step 6 is also confirmed by step 7 which then transmits a copy to the CA server 321. None of this relates to the subject matter at issue in claim 6.

Further, it is submitted that, even if the Examiner's reliance upon steps 7 and 8 to argue anticipation was not in error, the disclosure of Oka still would not anticipate because:

(i) step 8 does not refer to "a signature for an electronic document" but, rather, refers to a signature on a certificate; and

(ii) the reference does not at all limit validation of signatures on documents to **only** those generated on documents **prior** to the certification of the public validation key.

The invention of claim 6 concerns validating signatures on documents wherein the signatures are generated prior to "certification of the public validation key". The citation from Oka refers to signatures **on** a certification and this is inconsistent with claim 6. Clearly the signature which is **on** a certification (see par [00200] of Oka) must occur at the time the certification is generated (not beforehand) and such does not relate to the claimed invention. Nowhere in any of the citations from the Oka reference is there any mention of the combination of claim 6: "calculating an electronic signature for an electronic document" and requiring that "only those signatures generated at a time prior to the certification of the public validation key are recognized as valid." The rejection does not and cannot find anything equivalent to this

recitation in the Oka reference. The rejection only references a signature for a certificate rather than the signature on a document generated prior to the time the public validation key is certified. See pars [0201] and [0202] of Oka.

The citation from the Oka reference makes no disclosure of signatures generated prior to the certification of a public validation key and, even if it did make such a disclosure, there would still be no disclosure of only recognizing as valid those signatures generated prior to the time of certification of the public validation key. Therefore, it is not understood how the rejection can be supported by the cited text and Figure 22 of Oka.

The Oka reference does not and cannot refer to the signature for an electronic document which is signed before the certification is generated. For all of these reasons the rejection of claim 6 must be overturned.

7A(ii). REJECTION OF INDEPENDENT CLAIM 18 UNDER SECTION 102 BASED ON OKA IS ALSO IN ERROR.

The Final Office Action rejects claim 18 for the same reasons set forth in the rejection of claim 6. See page 4 of the office action. However, application of the Oka reference under Section 102 to claim 18 also results in deficiencies that render the rejection incorrect. The method of claim 18, like claim 6, requires **a certification of the public validation key wherein**

"only those signatures generated at a time prior to the certification of the public validation key are recognized as valid."

Again, the final office action does not account for the word "only" which requires that, for a signature to be valid, the signature must be generated prior to the time that the public validation key is certified. Reliance upon the Oka reference at page 12 (par 193) and Figure 22 is misplaced. Step 8 of Oka (par. [0201]) only concerns validation of a signature on a received public key certificate. Without support for doing so, the rejection concludes that because step 8 determines whether a signature on a public key certificate is valid, and step 9 (par. [0202]) sends a signed certificate to the registration authority, the terms of the above-quoted recitation are met. Yet this is not what claim 6 requires.

Claim 18 does not relate to step 9 of Oka (par [0202] - sending "a signed certificate to the registration authority"). Instead, the above recitation refers to signatures generated on documents prior to the *certification of the public validation key.* On the other hand, step 5 of Oka specifies that the "signature generation instruction" is command and message data *for a certificate to be generated* (see par 198); and step 6 expressly states that this same instruction is executed. Thus **the certificate is generated in step 6.** The fact that the certificate is generated in step 6 is also confirmed by step 7 which then transmits a copy to the CA server 321. None of this relates to the subject matter at issue in claim 18.

Further, the disclosure of Oka cannot anticipate because:

(i) step 8 does not refer to "a signature for an electronic document" but, rather, refers to a signature on a certificate; and

(ii) the reference does not at all limit validation of signatures on documents to **only** those generated on documents **prior** to the certification of the public validation key.

The invention of claim 18 concerns validating signatures on documents wherein the signatures are generated prior to "certification of the public validation key". The citation from Oka refers to signatures **on** a certification and this is inconsistent with claim 6.

Nowhere in any of the citations from the Oka reference is there any mention of the combination of claim 18: "calculating at least one electronic signature for at least one electronic document" and requiring that "only those signatures generated at a time prior to the certification of the public validation key are recognized as valid." The rejection does not and cannot find anything equivalent to this recitation in the Oka reference. The rejection only references a signature for a certificate rather than the signature on a document generated prior to the time the public validation key is certified. See pars [0201] and [0202] of Oka.

The citation from the Oka reference makes no disclosure of signatures generated prior to the certification of a public validation key and, even if it did make such a disclosure, there would still be no disclosure of only recognizing as valid those signatures generated prior to the time of certification of the public validation key. Therefore, it is not understood how the rejection can be supported by the cited text and Figure 22 of Oka.

In conclusion, the Oka reference does not and cannot refer to the signature for an electronic document which is signed before the certification is generated. For all of these reasons the rejection of claim 18 must be overturned.

7B. REJECTION OF THE DEPENDENT CLAIMS 8, 10, 12, 14, 16, 20, 22 AND 23 AS ANTICIPATED BY OKA UNDER SECTION 102 IS IN ERROR.

7B(i) REJECTION OF DEPENDENT CLAIM 8 UNDER SECTION 102 BASED ON OKA IS ALSO IN ERROR.

According to Claim 8, when certifying the public validation key, a reference to the electronic document is included in addition to a user identifier and the public validation key. The rejection has cited par [0011] of Oka for disclosing what a typical public key certificate includes, but that paragraph does not indicate that any reference is made, in the step of "performing a certification of the public key" to a specific electronic document for which the public key might be used. So it is not understood why par [0011] is cited to support rejection of claim 8 under Section 102. Furthermore, reference should be made to pars [0099] – [0102] of Oka which provide an explanation as to how the prior art certificate authority operates. Note, specifically, these passages do not make any reference to identification of any specific document during the process of issuing a public key certificate. The rejection must be overturned.

7B(ii) REJECTION OF DEPENDENT CLAIM 10 UNDER SECTION 102 BASED ON OKA IS ALSO IN ERROR.

The method of claim 10, which depends from claim 8, further requires that "an implementation of the reference is performed by a calculation of a hash value for the electronic document." In this regard the rejection refers to Oka at page 1, par. [0012], but this citation does not refer to use of a hash value for the document. Reference to Fig. 1 of Oka does not compensate for this deficiency because that Figure does not associate a document with the

certificate. It is noted that while that figure includes the text "ENTIRE MESSAGE" that text is part of the digital signature and not the same as appellants' recited "electronic document". Nor does it reference an electronic document. Further, the invention is not simply use of a hash value, but is a combination of features including those recited in claims 6 and 8. The combination is not taught or suggested. Removal of the rejection is requested.

7B(iii) REJECTION OF DEPENDENT CLAIM 12 UNDER SECTION 102 BASED ON OKA IS ALSO IN ERROR.

The method according to Claim 12 requires, following calculation of the signature and prior to its transfer to a recipient, that

"a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document."

At the outset, it is noted that the recited "validation" is in addition to the "certification of the public validation key" as recited in claim 6; and the validation of claim 12 is performed by the author of the document before transfer of the signature to the recipient. To reject claim 12 the Examiner cites pars [0201] – [0203] of Oka, but this is not useful because, as stated in paragraph [0200] the CA (not the author) checks whether the signed public key certificate is valid. The recited "author" cannot be read on the "end entity 300" because as best understood the rejection reads the recited "recipient" to whom the document is transferred on the end entity 300 of Figure 22. For these reasons the features of claim 12 and claim 6 from which it depends cannot be consistently read upon the Oka reference. The subject matter of claim 12 is not disclosed in the prior art and the rejection must be overturned.

7B(iv) REJECTION OF DEPENDENT CLAIM 14 BASED ON OKA UNDER SECTION 102 IS IN ERROR.

According to Claim 14, following calculation of the signature and prior to its transfer to a recipient, "a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document."

As argued for claim 12, at the outset, it is noted that the recited "validation" is in addition to the "certification of the public validation key" as recited in claim 6; and the validation of claim 14 is performed by the author of the document before transfer of the signature to the recipient. To reject claim 14 the Examiner cites pars [0201] – [0203] of Oka, but this is not useful because, as stated in paragraph [0200] the CA (not the author) checks whether the signed public key certificate is valid. The recited "author" cannot be read on the "end entity 300" because as best understood the rejection reads the recited "recipient" to whom the document is transferred on the end entity 300 of Figure 22. For these reasons the features of claim 14 and claim 6 from which it depends cannot be consistently read upon the Oka reference. The subject matter of claim 14 is not disclosed in the prior art and the rejection must be overturned.

7B(v) REJECTION OF DEPENDENT CLAIM 16 AS ANTICIPATED BY OKA UNDER SECTION 102 IS IN ERROR.

According to Claim 16, following calculation of the signature and prior to its transfer to a recipient, "a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document."

As argued for claims 12 and 14, it is again noted that the recited "validation" is in addition to the "certification of the public validation key" as recited in claim 6; and the validation of claim 16 is performed by the author of the document before transfer of the signature to the recipient. To reject claim 16 the Examiner cites pars [0201] – [0203] of Oka, but this is not useful because, as stated in paragraph [0200] the CA (not the author) checks whether the signed public key certificate is valid. The recited "author" cannot be read on the "end entity 300" because as best understood the rejection reads the recited "recipient" to whom the document is transferred on the end entity 300 of Figure 22. For these reasons the features of claim 16 and claim 6 from which it depends cannot be consistently read upon the Oka reference. The subject matter of claim 16 is not disclosed in the prior art and the rejection must be overturned.

7B(vi) REJECTION OF DEPENDENT CLAIM 20 UNDER SECTION 103 BASED ON OKA IS IN ERROR.

According to Claim 20, "when certifying the public validation key, at least one reference to the electronic document, of which there is at least one, is included in addition to a user identifier and the public validation key." As done for claim 6, the rejection has cited par [0011] of Oka for disclosing what a typical public key certificate includes, but that paragraph does not indicate that any reference is made, in the step of "performing a certification of the public key" to a specific electronic document for which the public key might be used. So it is not understood why par [0011] is cited to support rejection of claim 20 under Section 102. Furthermore, reference should be made to pars [0099] – [0102] of Oka which provide an explanation as to how the prior art certificate authority operates. Note, specifically, these passages do not make any reference to identification of any specific document during the process of issuing a public key certificate. Reversal of the rejection of claim 8 is requested.

7B(vii) REJECTION OF DEPENDENT CLAIM 22 AS ANTICIPATED BY OKA UNDER SECTION 102 IS IN ERROR.

The method of claim 22, which depends from claim 20, further requires that "an implementation of the reference, of which there is at least one, takes place by means of a calculation of a hash value for the electronic document, of which there is at least one."

In this regard, as per the rejection of claim 10, the rejection of claim 22 also refers to Oka at page 1, par. [0012], but this citation does not refer to use of a hash value for the document. Reference to Fig. 1 of Oka does not compensate for this deficiency because that Figure does not associate a document with the certificate. It is noted that while that figure includes the text "ENTIRE MESSAGE" that text is part of the digital signature and not the same as appellants' recited "electronic document". Nor does it reference an electronic document. Further, the invention is not simply use of a hash value, but is a combination of features including those recited in claims 6 and 8. The combination is not taught or suggested. Removal of the rejection is requested.

7B(viii) REJECTION OF DEPENDENT CLAIM 23 UNDER SECTION 102 BASED ON OKA IS ALSO IN ERROR.

The method according to Claim 23 also requires, following calculation of the signature and prior to its transfer to a recipient, that

"a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document."

As argued for claims 12, 14 and 16, it is once more noted that the recited "validation" is in addition to the "certification of the public validation key" as recited in claim 6; and the validation of claim 12 is performed by the author of the document before transfer of the signature to the recipient. To reject claim 12 the Examiner cites pars [0201] – [0203] of Oka, but this is not useful because, as stated in paragraph [0200] the CA (not the author) checks whether the signed public key certificate is valid. The recited "author" cannot be read on the "end entity 300" because as best understood the rejection reads the recited "recipient" to whom the document is transferred on the end entity 300 of Figure 22. For these reasons the features of claim 23 and claim 6 from which it depends cannot be consistently read upon the Oka reference. The subject matter of claim 23 is not disclosed in the prior art and the rejection must be overturned.

7C. CONCLUSIONS

Argument has been presented to demonstrate that all of the rejections under Section 103 are deficient and that the dependent claims further distinguish over the prior art. The Examiner has argued rejections when claimed features are absent from the references and not suggested by the prior art. The Examiner has written argument "as though" cited text contains the claimed subject matter, but a plain reading of the cited prior art text clearly shows that the rejections are without basis. Accordingly, none of the rejections can be sustained. For all of the above-argued reasons, all of the rejections should be overturned and the claims should be allowed.

8. APPENDICES

An appendix containing a copy of the claims involved in this appeal is provided herewith. No evidence appendix or related proceedings appendix is provided because no such evidence or related proceeding is applicable to this appeal.

Respectfully submitted,

Dated: Sept. 2, 2009

By: Janet D. Hood

Janet D. Hood
Registration No. 61,142
(407) 736-4234

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, New Jersey 08830

9. APPENDIX OF CLAIMS ON APPEAL

6. A method for generating and/or validating electronic signatures, the method comprising:

generating an asymmetrical key pair which includes a private signature key and a public validation key;

calculating an electronic signature for an electronic document by means of the private signature key and by applying a predeterminable signature function; and

performing a certification of the public validation key wherein, when validating, only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.

8. The method according to Claim 6, wherein, when certifying the public validation key, a reference to the electronic document is included in addition to a user identifier and the public validation key.

10. The method according to Claim 8, wherein an implementation of the reference is performed by a calculation of a hash value for the electronic document.

12. The method according to Claim 6, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.

14. The method according to Claim 8, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.

16. The method according to Claim 10, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.

18. A method for generating and/or validating electronic signatures, the method comprising:

generating an asymmetrical key pair which includes a private signature key and a public validation key;

calculating at least one electronic signature for at least one electronic document by means of the private signature key and by applying a predeterminable signature function; and

following calculation of the electronic signature, of which there is at least one, carrying out a certification of the public validation key wherein only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.

20. The method according to Claim 18, wherein, when certifying the public validation key, at least one reference to the electronic document, of which there is at least one, is included in addition to a user identifier and the public validation key.

22. The method according to Claim 20, wherein an implementation of the reference, of which there is at least one, takes place by means of a calculation of a hash value for the electronic document, of which there is at least one.

23. The method according to Claim 18, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, of which there is at least one, in order to verify an action of intent which is expressed by the electronic document, of which there is at least one.

10. EVIDENCE APPENDIX - 37 CFR 41.37(c) (1) (ix)

None

11. RELATED PROCEEDINGS APPENDIX - 37 CFR 41.37(c) (1) (x)

None